Nina Eisenberg (SBN 305617)
neisenberg@edelson.com
EDELSON PC
123 Townsend Street
San Francisco, California 94107
Tel: 415.212.9300
Fax: 415.373.9435

Robert C. Schubert (SBN 62684)
rschubert@sjk.law
Noah M. Schubert (SBN 278696)
nschubert@sjk.law
Kathryn Y. Schubert (SBN 265803)
kschubert@sjk.law
SCHUBERT JONCKHEER & KOLBE LLP
Three Embarcadero Center, Suite 1650
San Francisco, California 94111
Tel: 415.788.4220
Fax: 415.788.0161

Attorneys for Plaintiffs and the Putative Classes

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

JASON COOPER and MEGHNA PARIKH, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

SLICE TECHNOLOGIES, INC., a Delaware corporation, and UNROLLME INC., a Delaware corporation,

Defendants.

Case No.: 3:17-cv-02340-LB

CONSOLIDATED CLASS ACTION COMPLAINT FOR:

(1) Violations of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*;
(2) Violations of the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*;
(3) Violations of California's Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*;
(4) Unjust Enrichment; and Privacy Violation Based on Intrusion.

DEMAND FOR JURY TRIAL

Plaintiffs Jason Cooper and Meghna Parikh bring this Consolidated Class Action Complaint and Demand for Jury Trial against Defendants Slice Technologies, Inc. and UnrollMe Inc., to stop their practice of unlawfully mining and selling data collected from the private emails of millions of unwitting consumers. Plaintiffs allege as follows upon personal knowledge as to themselves and their own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by their attorneys.

NATURE OF THE ACTION

1. While millions of Americans have come to rely on email as a primary form of communication for their business and personal lives, their inboxes are increasingly being bogged down with the over 260 billion spam emails and advertisements sent daily. Defendant UnrollMe sought to capitalize on these frustrations and, in 2011, was founded purportedly to "clean up your inbox."[1]

2. Since its inception, Defendant UnrollMe has held itself out as a free web service with the sole purpose of allowing users to easily unsubscribe from mailing lists, newsletters and other unwanted emails.

3. Under the disguise of being a consumer friendly "email management" service, UnrollMe was able to mislead millions of consumers into granting them virtually unfettered access into their private and sensitive email inboxes. That is because users need to grant UnrollMe access to their email accounts (such as Gmail or Outlook) so that UnrollMe can identify and unsubscribe users from any unwanted messages. What UnrollMe does not draw attention to is that once it gets access to users' inboxes, it actually scans their emails, extracts a variety of data points, and then, through its parent company Defendant Slice Technologies, Inc. (doing business as Slice Intelligence), sells that data to third parties seeking to profile and target UnrollMe users. The New York Times recently reported one particular instance where Slice gathered data from thousands of UnrollMe users' emails who used the Lyft ridesharing service and then sold that highly valuable

[1] UnrollMe, https://unroll.me (last visited Apr. 26, 2017).

data to Uber (Lyft's largest competitor). With that information, Uber was able to gain a competitive edge at the expense of UnrollMe users' privacy.

4. Defendants did not adequately disclose to consumers the true purpose for why they seek access to UnrollMe users' emails for an important and obvious reason: few (if any) consumers would knowingly hand over complete access to their private emails to a company that would invasively scour through them and then sell the data they gather about you to whoever would pay the most.

5. In the end, Defendants misused the limited permission consumers granted to UnrollMe and unlawfully profited from it. Accordingly, this putative class action seeks (i) to prevent Defendants' unlawful interception and reading of consumers' emails, (ii) damages, including statutory and punitive damages, for violations under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.* ("ECPA"), Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.* ("SCA"), and California's Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.* ("CIPA").

PARTIES

6. Plaintiff Jason Cooper is a natural person and citizen and resident of the State of Michigan.

7. Plaintiff Meghna Parikh is a natural person and citizen and resident of the State of California.

8. Defendant Slice Technologies, Inc. is a corporation existing under the laws of the State of Delaware, with its principal place of business located at 800 Concar Drive, San Mateo, California 94402. Defendant Slice conducts business throughout this District, the State of California, and the United States.

9. Defendant UnrollMe Inc. is a corporation existing under the laws of the State of Delaware, with its principal place of business located at 222 Broadway, New York, New York 10038. Defendant UnrollMe is a subsidiary of Defendant Slice. Defendant UnrollMe conducts business throughout this District, the State of California, and the United States.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 because this action arises under the ECPA and SCA, which are federal statutes. This Court also has supplemental jurisdiction over Plaintiff Parikh's state law claims under 28 U.S.C. § 1367(a) because they are so related to her federal claims that they form part of the same case or controversy under Article III of the United States Constitution.

11. This Court has personal jurisdiction over Defendant Slice because it is headquartered in this District, conducts significant business in this District, and the unlawful conduct alleged in this Complaint occurred in and emanated from this District. This Court has personal jurisdiction over Defendant UnrollMe because it conducts significant business in this District, enters into contracts in this District, and the unlawful conduct alleged in this Complaint occurred in and emanated from this District.

12. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant Slice maintains its headquarters and principal place of business in this District and a substantial part of the events giving rise to Plaintiffs' Complaint occurred in this District.

INTRADISTRICT ASSIGNMENT

13. Pursuant to Civil Local Rule 3-2(d), this case should be assigned to the San Francisco Division.

FACTUAL BACKGROUND

I. UnrollMe's "Email Management" Service Serves as a Backdoor Data Collection Tool for Data Miner, Slice Intelligence.

14. In 2011, UnrollMe was launched purportedly to help consumers tackle the deluge of unwanted emails cluttering their inboxes. By signing up with UnrollMe, consumers could purportedly rid their email inboxes of junk by using UnrollMe's "email management" service to mass unsubscribe from spam messages and to group categories of emails into a single email digest that would be sent to the user daily. In exchange, UnrollMe could display daily advertisements to users via the digests and offer them new productivity products or services over time.

15. In 2014, Defendant Slice purchased UnrollMe. While Slice Intelligence is not a household name, it has become a major data mining company that claims to turn data from over 4.2 million online shoppers "into actionable insights, furnishing brands and retailers with the answers to essential questions about digital commerce . . . ."[2]

16. Slice gathers its data using "technology that automatically identifies e-receipts within [email] inboxes, extract[ing] every available data point about every purchase at the item level" from a "panel" of online shoppers.[3]

17. Slice uses this information culled from consumers' e-receipts to build market research products that analyze and track consumer trends. Slice's technology "measures all online purchases, using the same methodology, tied to the same consumer, including that consumer's historical purchase patterns to reveal loyalty and switching behavior…."[4] Slice then sells this user information to businesses seeking insights into consumer behavior and seeking to gain a competitive advantage.

18. In November 2014, Slice purchased UnrollMe for an undisclosed sum. Prior to the acquisition, UnrollMe was a free service that generated revenue through advertisements shown to its 1.3 million users.[5] And while UnrollMe remained and continues to be a free service, it changed how it makes money. Rather than selling ad space, it now sells access to its unwitting users' email accounts. By leveraging Slice's technology, Slice and UnrollMe riffle through users' inboxes and inventory valuable emails, including receipt data that Slice can sell to businesses seeking to track consumer habits.

19. Slice's access to the millions of UnrollMe's users' inboxes provides it with the data

---

[2] *Methodology*, Slice Intelligence, https://intelligence.slice.com/methodology/ (last visited Apr. 26, 2017).

[3] *Id.*

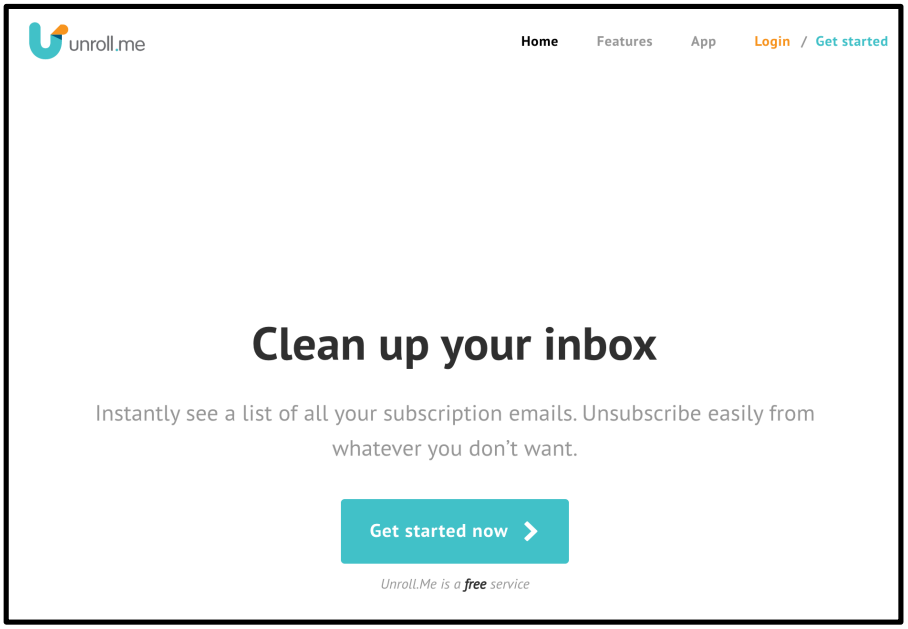
[4] *Id.*

[5] Ingrid Lunden, *Post Rakuten Acquisition, Slice Buys Unroll.Me to Add Email List Control to Its Shopping App*, TechCrunch (Nov. 24, 2014), https://techcrunch.com/2014/11/24/rakuten-slice-buys-unroll-me/.

it recognizes is "of unparalleled quality, granularity and comprehensiveness. Data is reported daily at the item level, by zip-code and across all retailers, all categories, on any and all devices which a purchase was made. This is high definition data."[6]

A. *Conspicuously absent from UnrollMe's registration process and marketing materials is any mention that Defendants will mine users' emails for valuable data.*

20. UnrollMe does not adequately disclose its true business model, recognizing that few (if any) consumers would knowingly hand over their private emails to a company if they knew the company would invasively scour through their messages for the purpose of selling their data to whoever would pay the most. As such, UnrollMe disguises itself as a friendly "email management" service in order to mislead consumers into signing up for it and, in turn, granting it access to their private email inbox. (*See* Figure 1, showing a screenshot of UnrollMe's marketing materials contained on its website.)

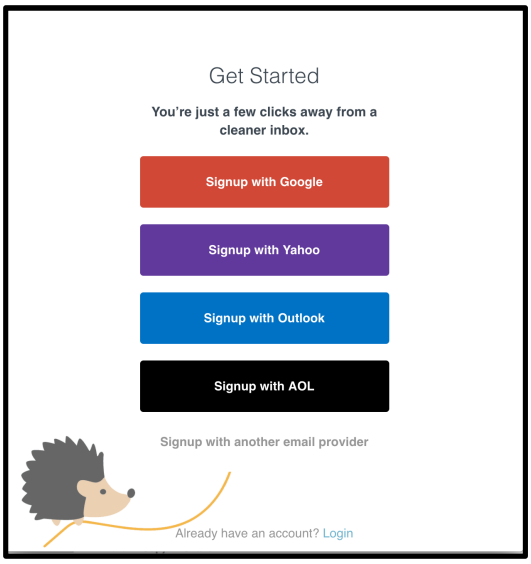


(**Figure 1.**)

21. Not surprisingly, nowhere during the sign-up process does UnrollMe disclose that it will scour users' emails for "valuable data points" and then sell that information through Slice. Instead, UnrollMe continues to present prospective users with advertisements about how UnrollMe

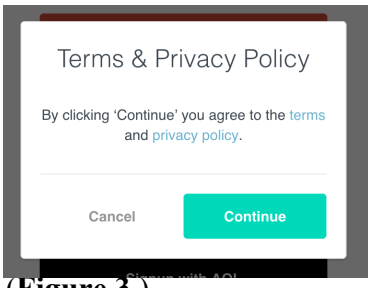
[6] *Id.*

is merely designed to allow users to get a "cleaner inbox." (*See* Figure 2, showing a screenshot of UnrollMe's registration process.)



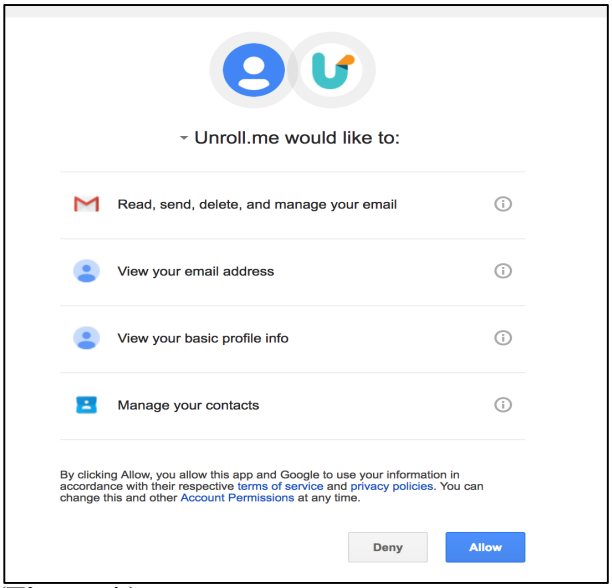
(**Figure 2.**)

22. If a prospective user continues with the sign-up process depicted above, UnrollMe will eventually display a link to its terms of use and privacy policy shown in Figure 3. However, as described in detail in Section II below, even there UnrollMe does not adequately disclose its true business model.



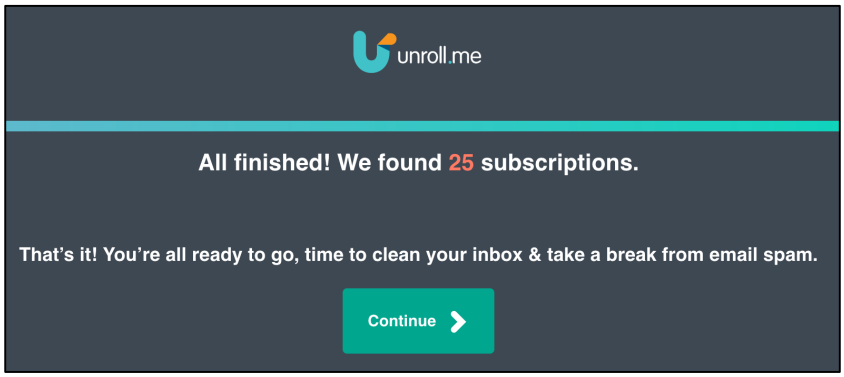
(**Figure 3.**)

23. For sake of completeness, the prospective user connecting UnrollMe to their Google email account, for example, would next be asked by Google if UnrollMe could receive certain "permissions" to access their email account. (*See* Figure 4, showing a screenshot of Google's permission screen for UnrollMe.)



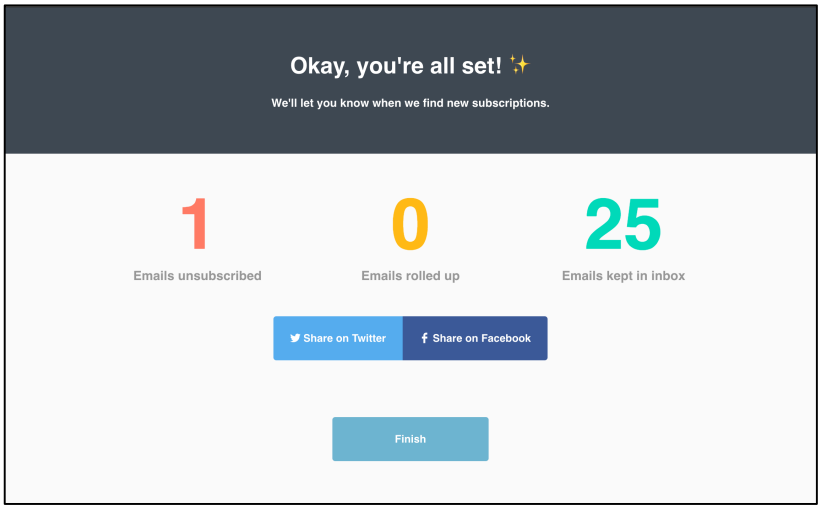
(**Figure 4.**)

24. If the prospective user selects "Allow," UnrollMe claims to conduct an initial search for subscription emails that the user can use UnrollMe to unsubscribe from. (*See* Figure 5, showing a screenshot of UnrollMe's graphical user interface.)



(**Figure 5.**)

25. As shown in Figure 5, UnrollMe claimed to have "found 25 subscriptions" that the user could unsubscribe from to "clean [their] inbox & take a break from email spam." After the user pressed continue and selected which emails to unsubscribe from, UnrollMe claimed that the user is "all set" and that the UnrollMe would continue into the future to "find new subscriptions" as shown in Figure 6, on the following page.



(**Figure 6.**)

B. *UnrollMe disguises itself as a friendly "email management" service to mislead consumers into signing up for it.*

26. As Figures 1–6 show, UnrollMe appears to be fairly straightforward. UnrollMe claims to declutter your email inbox and, in line with that, asks for permission specifically to access consumers' email accounts to "find new subscriptions" from which they can use the service to unsubscribe from.

27. Unfortunately, claiming to be a friendly and useful email service is just a disguise to get access to the valuable information contained in your emails. Defendants overstep the level of permission consumers grant to UnrollMe and secretly enroll them in Slice's "online panel of shoppers"—where they surreptitiously scan consumers' emails, harvesting them for valuable data, and sell that data to the highest bidder.

28. In fact, a well-respected tech journalist, Mike Isaac of The New York Times, recently reported one instance where these supposedly "commercial transactional messages" were collected by Defendants and then auctioned off. Consumers who signed up for UnrollMe and had used the Lyft ridesharing application had their private emails taken and sold to Uber—the notorious competitor to Lyft. To be clear: Uber was paying top dollar for the private emails of thousands of Lyft users that were collected by Defendants while consumers were in the dark.

II. Defendants Exceeded the Limited Permission Given to UnrollMe to Secretly Read and Collect Data from Consumers' Private Emails.

29. Defendants went to great length to distance UnrollMe from the Slice. Reasonable consumers viewing UnrollMe's marketing materials and going through the UnrollMe sign up process think that they are simply signing up for a service that will help them unsubscribe from unwanted spam emails. What consumers don't know—and what Defendants have thus far successfully obfuscated—is that by giving UnrollMe access to their emails for the limited purpose of unsubscribing from spam, they have let the fox into the henhouse. By convincing consumers to trust UnrollMe, Slice was able to gain access to millions of consumers' private emails, from which it analyzes, collects, and sells information to third parties.

A. *UnrollMe recognizes that its disclosures were inadequate.*

30. According to UnrollMe's CEO and Co-Founder, "while [UnrollMe] tr[ied] [its] best to be open about [its] business model, recent customer feedback tells me [they] weren't explicit enough."[7] He continued, "[s]ure we have a Terms of Service Agreement and a plain-English Privacy Policy that our users agree they have read and understand before they even sign up, but the reality is most of us - myself included – don't take the time to thoroughly review them."[8]

31. In its Privacy Policy, UnrollMe attempts to disclose that by using its service it *may* collect data from certain user emails. For instance, UnrollMe states:

> **Our Collection and Use of Non-Personal Information**
>
> We also collect non-personal information − data in a form that does not permit direct association with any specific individual. We may collect, use, transfer, sell, and disclose non-personal information for any purpose. For example, when you use our services, we may collect data from and about the "commercial electronic mail messages" and "transactional or relationship messages" (as such terms are defined in the CAN-SPAM Act (15 U.S.C. 7702 et. seq.) that are sent to your email accounts. We collect such commercial transactional messages so that we can better understand

[7] Jojo Hedaya, *We Can Do Better*, UNROLL.ME (Apr. 23, 2017), http://blog.unroll.me/we-can-do-better/.

[8] *Id.*

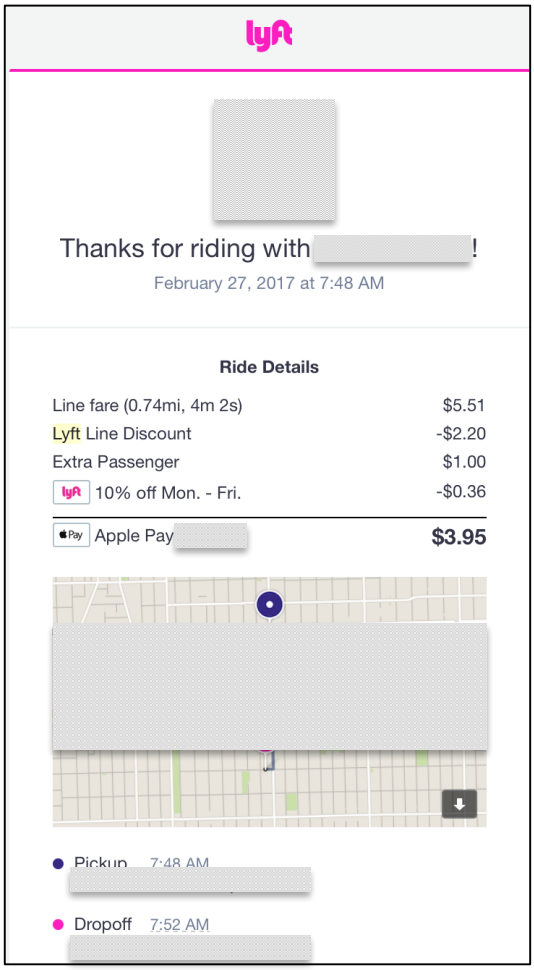
> the behavior of the senders of such messages, and better understand our customer behavior and improve our products, services, and advertising. We may disclose, distribute, transfer, and sell such messages and the data that we collect from or in connection with such messages; provided, however, if we do disclose such messages or data, all personal information contained in such messages will be removed prior to any such disclosure.
>
> We may collect and use your commercial transactional messages and associated data to build anonymous market research products and services with trusted business partners. If we combine non-personal information with personal information, the combined information will be treated as personal information for as long as it remains combined.
>
> Aggregated data is considered non-personal information for the purposes of this Privacy Notice.[9]

32. However, even reading the disclosure above in a light most favorable to UnrollMe (which is deficient), it is still inconsistent with UnrollMe's marketing materials and representations about what the service is and why consumers should sign up for it. As such, Defendants do not obtain proper consent for their clandestine business model of mining UnrollMe users' emails in order for Slice to sell their data. Put another way, UnrollMe heavily emphasizes throughout its marketing materials and website—including in the screenshots shown above—that it needs access to users' email accounts *specifically* to search for subscription emails for the purpose of "rolling-up" or unsubscribing from such emails. Consumers understand that tradeoff: give UnrollMe access to their personal (or business) email accounts in exchange for UnrollMe getting rid of annoying emails and potentially showing them advertisements or other productivity services or products. UnrollMe hides the fact that it actually scours user emails for valuable data and then sells that user data through its parent company, Slice.

33. The New York Times article mentioned above revealed that one company in particular that buys this supposedly anonymous email data is Uber, a company that's becoming best known for its alleged invasive tracking of individuals and large-scale data mining practices. However, it is worth noting that completely anonymous emails are likely of little value to a company such as Uber. Instead, these emails typically only have value when they have as many of

[9] *Privacy Policy*, UnrollMe, https://unroll.me/legal/privacy/ (last visited Apr. 26, 2017).

these details intact, meaning these supposedly "transactional" emails likely reveal tremendous amounts of information about UnrollMe's users. For instance, the screenshot below shows the contents of a typical Lyft "transactional" email that shows a picture and the name of the driver, the date, time, and distance of the trip, the total fare, and the precise pickup and drop-off locations. (*See* Figure 7, showing an example of an email receipt for a Lyft ride.)



(**Figure 7**.)

34. Even assuming Defendants performed *some* level of anonymization (*e.g.*, removing first and last names and email addresses), it likely wasn't sufficient. Researchers have revealed the ease in which particular people can be identified from purportedly anonymized data sources.[10] This

[10] *See* Mudhakar Srivatsa and Mike Hicks. 2012. *Deanonymizing mobility traces: using social network as a side-channel*. In Proceedings of the 2012 ACM conference on Computer and

is particularly easy to accomplish when the dataset is taxi trips, like the Lyft data Defendants sold. In 2014, researchers analyzed a taxi dataset released by the city of New York. As The Guardian reported:

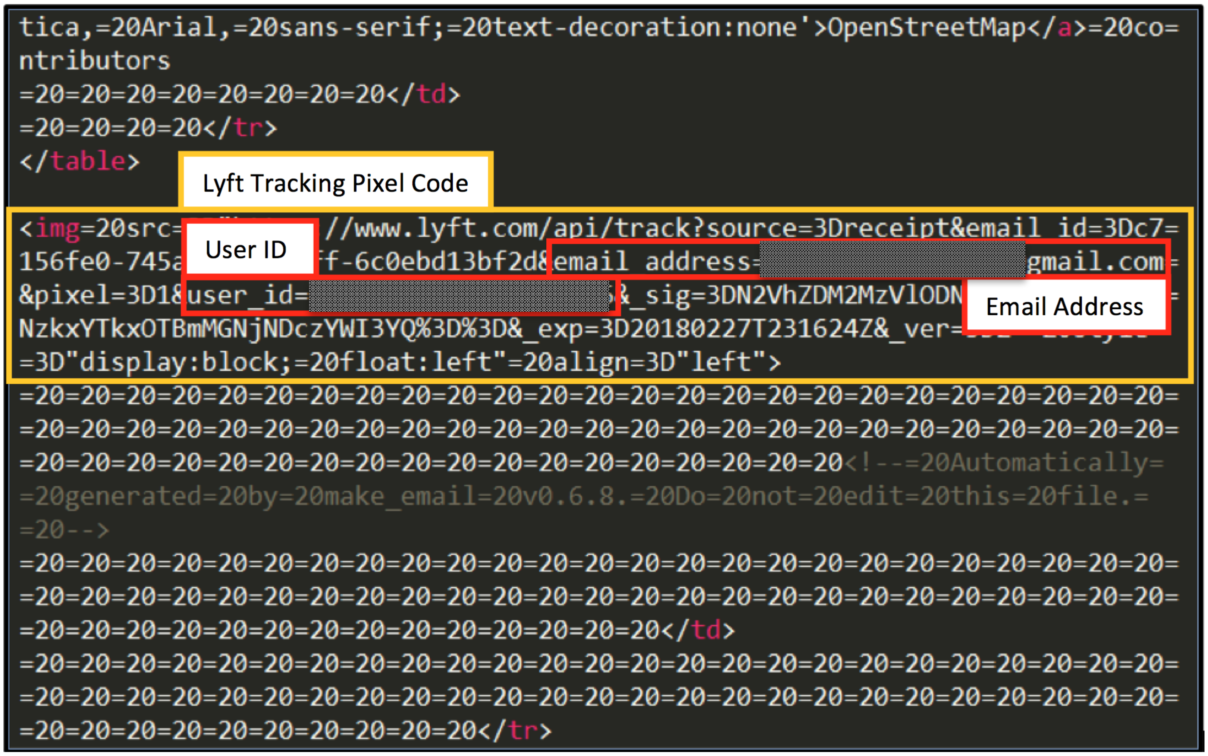
> New York City has released data of 173m individual taxi trips – but inadvertently made it "trivial" to find the personally identifiable information of every driver in the dataset.
>
> The data could let malicious parties work out the home addresses of drivers, uncover their income, and retrace their movements across the city. But even without that, some users worry that the dataset also exposes passenger information to the world – which could reveal personal information about their journey points and times.[11]

35. Indeed, a Lyft email receipt can reveal that information even if Defendants attempted some anonymization technique, they may have overlooked information unique to the consumer. Behind every Lyft email are unique identifiers that can identify each Lyft user. Figure 8 on the following page, shows an excerpt of code in a Lyft email receipt containing unique identifiers that can identify the individual rider.

* * *

communications security (CCS 2012). ACM, New York, NY, USA, 628-637. DOI: http://dx.doi.org/10.1145/2382196.2382262; *see also* Anonymous *Usage of Location-Based Services through Spatial and Temporal Cloaking*. Marco Gruteser and Dirk Grunwald. MobiSys 2003.

[11] *New York taxi details can be extracted from anonymised data, researchers say | Technology | The Guardian*, https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn (last visited Apr. 26, 2017).



(**Figure 8**.)

36. The reputation of Uber, the company Defendants sold consumers' email data to, is also illuminating when considering the extent of any "anonymization." Uber has reportedly violated consumers' privacy when it, for instance, "Allegedly Stalked Users For Party-Goers' Viewing Pleasure" through the use of a "God mode," where it watched customers' trips in real time;[12] "secretly identif[ied] and tagg[ed] iPhones even after its app had been deleted and the devices erased,"[13] and updated its app to require consumers to allow Uber to track them even when not using the app. That last practice led to Senator Al Franken writing a sternly worded letter saying that "consumers have a right to clear and comprehensive information about what data are being collected about them, how the data are being treated, and with whom the data are being

---

[12] *'God View': Uber Allegedly Stalked Users For Party-Goers' Viewing Pleasure (Updated)*, https://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure/#2bde726e3141 (last visited Apr. 26, 2017).

[13] *Uber's C.E.O. Plays With Fire - The New York Times*, https://www.nytimes.com/2017/04/23/technology/travis-kalanick-pushes-uber-and-himself-to-the-precipice.html?_r=1 (last visited Apr. 26, 2017).

shared."[14] Given Uber's reported proclivity for invasive tracking, it likely has the means to re-identify the Lyft data Defendants sold to it.

37. Ultimately, the millions of consumers who registered for UnrollMe's email "management service" had their privacy and trust violated. Consumers placed considerable trust in UnrollMe to access to their private and sensitive communications and UnrollMe, operating as a disguise for its parent, Slice, betrayed that trust by secretly combing through emails *en masse* and selling collected emails to anyone willing to pay.

FACTS RELATING TO PLAINTIFF JASON COOPER

38. Plaintiff Jason Cooper registered for an UnrollMe account in or around 2015. Before signing up for UnrollMe, Plaintiff Cooper saw UnrollMe's representations that UnrollMe would require access to his email account so that it could identify "subscription" emails that filled his email inbox. Plaintiff Cooper did not know that Defendants would actually use the access that UnrollMe acquired to read the contents of his emails and then sell that email data to third parties.

39. While Plaintiff Cooper had UnrollMe, he sent and received thousands of emails. Defendants were not a party or an intended party to those emails (except for any emails UnrollMe may have sent automatically as a part of its service). In addition, neither UnrollMe or Slice (a company Plaintiff had never even heard of) were intended recipients of any of his emails, except for any emails UnrollMe may have sent automatically as a part of its service.

40. Unbeknownst to Plaintiff Cooper (and without his informed consent), Defendants intercepted and read the contents of his private emails. For instance, Defendants read Plaintiff Cooper's emails to identify "transactional" messages so that it could mine them for data and then sell that data to third parties.

41. In addition, and unbeknownst to Plaintiff Cooper, Defendants exceeded the authorization UnrollMe had to Plaintiff Cooper's Gmail account, accessed his emails, read the

[14] *Sen. Franken Presses Uber to Upgrade Privacy Policy, Protect Users' Sensitive Location Data | Al Franken | Senator for Minnesota*, https://www.franken.senate.gov/?p=press_release&id=3593 (last visited Apr. 26, 2017).

contents of those emails to look for "transactional" messages that it could collect and sell to third parties.

42. At no time did Plaintiff Cooper consent to Defendants' interception, reading, monitoring, or use of the contents of the emails he sent or received for any purpose other than "cleaning up" his inbox.

FACTS RELATING TO PLAINTIFF MEGHNA PARIKH

43. Plaintiff Meghna Parikh registered for an UnrollMe account in or around 2015. Upon registering for an account, Plaintiff Parikh granted UnrollMe access to her Gmail account.

44. Plaintiff Parikh receives, stores, and sends sensitive and personal information on her Gmail account.

45. Based on Defendant's marketing materials, Plaintiff Parikh believed that Defendant UnrollMe was an email management system that would help eliminate junk mail and declutter her Gmail inbox. Before and while using UnrollMe's service, Plaintiff Parikh did not know or believe that Defendants would collect, transfer, disclose, and/or sell information contained in her Gmail emails.

46. Plaintiff Parikh did not know that Defendant UnrollMe was owned by Defendant Slice, a data mining company. Plaintiff never granted Defendant Slice access to her Gmail account, and Plaintiff did not know that Defendant Slice had access to her Gmail account and/or the emails and personal information contained therein.

47. Unbeknownst to Plaintiff Parikh, Defendants read and sold or otherwise disclosed the contents of her Gmail emails, including personally identifiable information specific to Plaintiff Parikh.

48. Plaintiff Parikh used Lyft's services while UnrollMe had access to her Gmail account. Plaintiff Parikh's Lyft receipts were sent to her Gmail account while UnrollMe had access to her account. Plaintiff Parikh believes that personally identifiable information in her Lyft receipts may have been sold to Uber by Defendant Slice.

49. Plaintiff Parikh did not consent to Defendants' interception, disclosure, transfer, or

sale of her personally identifiable information.

50. Plaintiff Parikh would not have granted Defendants access to her Gmail account if Defendants had properly disclosed to her its practice of monitoring, collecting, transferring and selling personal information.

CLASS ALLEGATIONS

51. Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23(b)(2) and (3) on behalf of themselves and two Classes and one Subclass of similarly situated individuals, defined as follows:

> **ECPA Class**: All individuals in the United States who (i) sent or received one or more emails (ii) where Defendants were not a party to the emails, and (iii) while they had UnrollMe installed.
>
> **SCA Class**: All individuals in the United States who (i) installed UnrollMe (ii) on email accounts where one or more emails were stored.
>
> **California Subclass**: All members of the ECPA or SCA Classes who reside in the State of California.

Excluded from the ECPA Class, SCA Class, and California Subclass (collectively the "Classes," unless otherwise indicated) are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and their current, former, purported, and alleged employees, officers, and directors; (3) counsel for Plaintiffs and Defendants; (4) persons who properly execute and file a timely request for exclusion from the Classes; (5) the legal representatives, successors, or assigns of any such excluded persons; and (6) all persons who have previously had claims similar to those alleged herein finally adjudicated or who have released their claims against Defendants.

52. **Numerosity**: The exact number of members in each of the Classes is unknown to Plaintiffs at this time, but on information and belief, there are tens of thousands of people in each of the Classes, making joinder of each individual member impracticable. Ultimately, members of the Classes will be easily identified through Defendants' records.

53. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Classes, and those questions

predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include but are not limited to the following:

(a) whether Defendants obtained adequate consent to intercept and/or access Plaintiffs' and the Classes' emails for the reasons discussed above;

(b) whether Plaintiffs and members of the Classes have a reasonable expectation of privacy in the information collected by Defendant UnrollMe;

(c) whether Defendants obtained adequate consent to intercept and/or access Plaintiffs' and the Classes' emails for only the purpose of identifying "subscription" emails;

(d) whether Defendants intercepted Plaintiffs' and the Classes' emails for purposes other than the identification of "subscription" emails;

(e) whether Defendants used the contents of Plaintiffs' and the Classes' emails for their benefit;

(f) whether Defendants accessed Plaintiffs' and the Classes' emails for purposes other than the identification of "subscription" emails;

(g) whether Defendants' access of Plaintiffs' and the Classes' emails for purposes other than the identification of "subscription" emails exceeded the authorization they were provided;

(h) whether Defendants' conduct violates the ECPA;

(i) whether Defendants' conduct violates the SCA;

(j) whether Defendants' conduct violates California's Invasion of Privacy Act;

(k) whether Defendants' conduct described herein has caused them to be unjustly enriched; and

(l) whether Plaintiffs and the members of the Classes are entitled to equitable relief as well as actual, statutory, and/or punitive damages as a result of Defendants' conduct.

54. **Typicality**: Plaintiffs' claims are typical of the claims of all the other members of the Classes. Plaintiffs and the members of the Classes sustained substantially similar damages as a result of Defendants' uniform wrongful conduct, based upon the same acts that Defendants made uniformly with Plaintiffs and the public.

55. **Adequate Representation**: Plaintiffs will fairly and adequately represent and protect the interests of the other members of the Classes. Plaintiffs have retained counsel with

substantial experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Classes.

56. **Policies Generally Applicable to the Classes**: Defendants have acted and failed to act on grounds generally applicable to Plaintiffs and the other members of the Classes, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Classes.

57. **Superiority**: This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Classes will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' actions. Thus, it would be virtually impossible for the individual members of the Classes to obtain effective relief from Defendants' misconduct. Even if members of the Classes could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court. Economies of time, effort, and expense will be fostered and uniformity of decisions ensured.

58. Plaintiffs reserve the right to revise the definitions of the Classes and Class Allegations based on further investigation, including facts learned in discovery.

FIRST CAUSE OF ACTION
Violations of the Electronic Communications Privacy Act
18 U.S.C. §§ 2510, *et seq*.
(On Behalf of Plaintiffs and the ECPA Class)

59. Plaintiffs incorporate by reference the foregoing allegations.

60. The ECPA prohibits any person from intentionally intercepting any electronic communication or from intentionally using, or endeavoring to use, the contents of any electronic communication while knowing or having reason to know that the information was obtained through the interception of an electronic communication. 18 U.S.C. § 2511(1) (a), (c), (d).

61. Defendants are each a "person" under the ECPA, which is broadly defined to include "any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

62. Emails are "electronic communications" under the ECPA, which are broadly defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate or foreign commerce . . . ." 18 U.S.C. § 2510(12).

63. Plaintiffs and the members of the ECPA Class sent or received "electronic communications" while having the UnrollMe installed.

64. Defendants intercepted, read, and used (and sought to use) the emails sent or received by Plaintiffs and each member of the ECPA Class between the time each such message was sent, on the one hand, and the time such message was read by the recipient. In doing so, Defendants used electronic, mechanical, or other devices (i.e., their UnrollMe code) to automatically acquire and read the content of the emails in the course of each such message's transmission.

65. Defendants intentionally used, or endeavored to use, the contents of these emails while knowing or having reason to know that the information was obtained through the interception of an electronic communication.

66. Defendants are neither parties to the emails sent or received by Plaintiffs and members of the ECPA Class, nor are they the intended recipients (except for any emails exchanged with UnrollMe as a part of the service).

67. Defendants' actions as complained of herein have been intentional, as evidenced by the design and implementation of their UnrollMe service.

68. No party to the electronic communications alleged herein consented to Defendants' interception or use of the contents of the electronic communications. Nor could they, because Defendants never sought to obtain consumers' consent for their practices exceeding the "subscription" email management.

69. Plaintiffs and members of the ECPA Class suffered harm as a result of Defendants' violations of the ECPA, and therefore seek (a) preliminary, equitable and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and the profits obtained by Defendants as a result of their unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(2)(B), whichever is greater, (c) punitive damages, and (d) reasonable costs and attorneys' fees.

SECOND CAUSE OF ACTION
Violation of the Stored Communications Act
18 U.S.C. §§ 2701, *et seq*.
(On Behalf of Plaintiffs and the SCA Class)

70. Plaintiffs incorporate by reference the foregoing allegations.

71. Defendants intentionally accessed without authorization or exceeded authorization to access a facility through which an electronic communication service is provided and obtained electronic communications while in electronic storage.

72. As described above, Defendants advertise UnrollMe as a service that helps consumers find and eliminate so-called "subscription" emails. Defendants do not disclose in UnrollMe's advertisements or marketing materials that consumers using UnrollMe are added to Slice's "panel" of online shoppers (through which Defendants obtain users' emails and sell data from them to third parties) but rather attempts to generally disclaim that in the UnrollMe Privacy Policy.

73. As such, to the extent Defendants obtained any authorization to access the emails of Plaintiffs and members of the SCA Class, Defendants exceeded the scope of that authorization by accessing emails for purposes other than the identification of "subscription" emails.

74. Plaintiffs' and members of the SCA Class's cloud based email accounts, including

Gmail, Hotmail, Yahoo email, and AOL email, are facilities under the SCA.

75. Plaintiffs' and members of the SCA Class's emails are electronic communications as defined by 18 U.S.C. § 2510 (12) because they are writings or the other transfer of data or intelligence that were sent or received over the internet, which affects interstate commerce.

76. And at the time Defendants accessed Plaintiffs' and the SCA Class's emails, the emails were in electronic storage. The emails were stored by the cloud email provider (*i.e.*, the electronic communication service) for future access by Plaintiffs and members of the SCA Class. That is, the cloud email providers kept the emails for the purpose of backup protection.

77. Defendants are neither parties to the emails sent or received by Plaintiffs and members of the SCA Class, nor are they the intended recipients (except for any emails exchanged with UnrollMe as a part of the service).

78. At all times, Defendants' actions as complained of herein have been intentional, as evidenced by the design and implementation of using their UnrollMe software as a backdoor for Slice's data mining practices.

79. Plaintiffs and members of the SCA Class have been aggrieved by Defendants' violations of the SCA, and therefore seek (a) preliminary, equitable and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and the profits obtained by Defendants as a result of their unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2707(c), whichever is greater, (c) punitive damages, and (d) reasonable costs and attorneys' fees.

THIRD CAUSE OF ACTION
Violation of California's Invasion of Privacy Act
Cal. Penal Code §§ 630, *et seq*.
(On Behalf of Plaintiff Parikh and the California Subclass)

80. Plaintiff Parikh incorporates by reference the foregoing allegations.

81. California's Invasion of Privacy Act ("CIPA") prohibits persons from intentionally, willfully and without the consent of all parties to the communication, or in any unauthorized manner, reading, or attempting to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being

sent from, or received at any place within California. Cal. Penal Code § 631.

82. CIPA also prohibits any person from using, or attempting to use, in any manner, or for any purpose, or communicating in any way, any information so obtained. CIPA further provides that any person who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above is punishable by fine or imprisonment. Cal. Penal Code § 631.

83. As described herein, Plaintiff Parikh and the California Subclass members authorized Defendant UnrollMe to access their email accounts for the limited purpose of providing email management services, and Defendant UnrollMe exceeded this authorization by reading the contents of their emails and using, attempting to use, and/or communicating such information to Defendant Slice and selling such information to unauthorized third parties.

84. As described herein, Plaintiff Parikh and the California Subclass members never consented to or authorized Defendant Slice to read, attempt to read, or learn the contents of their emails. Without the consent of Plaintiff Parikh and the California Subclass members, Defendant Slice used, attempted to use, communicated, and/or sold such information to third parties.

85. Defendants are neither parties to the emails sent or received by Plaintiff Parikh and the California Subclass, nor are they the intended recipients (except for any emails exchanged with UnrollMe as a part of the service).

86. As described herein, Defendants UnrollMe and Slice aided, agreed with, employed, and/or conspired with each other to read, attempt to read, or learn the contents of Plaintiff Parikh's and the California Subclass members' emails by using Defendant UnrollMe's email management service to gather consumer information for Defendant Slice.

87. At all times, Defendants' actions complained of herein have been intentional and willful, as evidenced by the design and implementation of using Defendant UnrollMe's email management service as a means for Defendant Slice to obtain user information and sell such information to third parties.

88. Plaintiff Parikh and the California Subclass members suffered harm as a result of

Defendants' violations of CIPA, and therefore seek (a) preliminary, equitable, and declaratory relief as may be appropriate, (b) the greater of five thousand dollars ($5,000) per violation and three times the amount of actual damages sustained, as authorized by Cal. Penal Code § 637.2, and (c) reasonable attorneys' fees and other litigation costs reasonably incurred.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Classes)

89. Plaintiffs incorporate by reference the foregoing allegations.

90. Absent Defendants' unauthorized monitoring, disclosure, or sale of UnrollMe users' personal information, Defendants would have had to pay Plaintiffs and each member of the Class monetary compensation in exchange for their valuable personal information and consumer habits. As such, Plaintiffs and other members of the Class conferred an improper windfall upon Defendants, which knew of the windfall and have unjustly retained such benefits.

91. As a direct and proximate result of Defendants' unjust enrichment, under principles of equity and good conscience, Plaintiffs and the Class are entitled to full disgorgement and restitution of all amounts by which Defendants were enriched through their unlawful or wrongful conduct.

FIFTH CAUSE OF ACTION
Privacy Violation Based on Intrusion
(On Behalf of Plaintiffs and the Classes)

92. Plaintiffs incorporate by reference the foregoing allegations.

93. Defendants, by collecting and disseminating Plaintiffs' and Class members' personal information and email contents without their knowledge, intentionally intruded into a realm in which Plaintiffs and Class members have a reasonable expectation of privacy.

94. Defendants are neither parties to the emails sent or received by Plaintiffs, nor are they the intended recipients (except for any emails exchanged with UnrollMe as a part of the service).

95. Defendants obtained unwanted access to Plaintiffs' and Class members' data, including but not limited to, the purchasing and travel habits of Plaintiffs and the Class members.

96. Defendants' intrusion into Plaintiffs' and Class members' privacy would be highly offensive to a reasonable person, because it occurred without Plaintiffs' or Class members' knowledge or consent.

97. By invading Plaintiffs' and the Class members' privacy, Defendants have obtained moneys which rightfully belong to Plaintiffs and the Class.

98. It would be inequitable and unjust for Defendants to retain these wrongfully obtained profits and benefits at Plaintiffs' and the Class members' expense.

99. Plaintiffs and the Class are entitled to restitution of the profits unjustly obtained (plus interest), as well as damages for Defendants' invasion of privacy.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Jason Cooper and Meghna Parikh, individually and on behalf of the Classes, pray for the following relief:

A. Certify this case as a class action on behalf of the Classes defined above, appoint Jason Cooper and Meghna Parikh as representatives for the Classes, and appoint their counsel as counsel for the Classes;

B. Declare that Defendants' actions, as described herein, violate the ECPA, and SCA;

C. Declare that Defendants' actions, as described herein, constitute unjust enrichment and a privacy violation based on intrusion;

D. Award injunctive relief as necessary to protect the interests of Plaintiffs and the members of the Classes, including, among other things, an order prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

E. Award equitable relief including, among other things, nonrestitutionary disgorgement, as necessary to prevent Defendants from profiting from the wrongful and unlawful acts described herein;

F. Award damages, including:

i. the greater of (a) the sum of actual damages suffered plus any profits Defendants earned through their unlawful conduct, and (b) the greater of

$100 per member of the ECPA Class, per day of Defendants' violations, or $10,000 per member of the ECPA Class, pursuant to 18 U.S.C. § 2520(c)(2);

ii. the greater of (a) the sum of actual damages suffered plus any profits Defendants earned through their unlawful conduct, and (b) $1,000 per member of the SCA Class, pursuant to 18 U.S.C. § 2707 (c); and

iii. the greater of (a) three times the amount of actual damages suffered plus any profits Defendants earned through their unlawful conduct, and (b) $5,000 per member of the California Subclass, pursuant to Cal. Penal Code §§ 637.2(a);

iii. punitive damages, where applicable, to Plaintiffs and the Classes in an amount to be determined at trial;

G. Award Plaintiffs and members of the Classes their reasonable litigation expenses and attorneys' fees;

H. Award Plaintiffs and members of the Classes pre- and post-judgment interest, to the extent allowable; and

I. Award such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

Respectfully submitted,

JASON COOPER and **MEGHNA PARIKH**, individually and on behalf of all others similarly situated,

Dated: July 10, 2017

By: */s/ Nina Eisenberg*
One of Plaintiffs' Attorneys

Nina Eisenberg (SBN 305617)
neisenberg@edelson.com
EDELSON PC
123 Townsend Street

San Francisco, California 94107
Tel: 415.212.9300
Fax: 415.373.9435

Robert C. Schubert (SBN 62684)
rschubert@sjk.law
Noah M. Schubert (SBN 278696)
nschubert@sjk.law
Kathryn Y. Schubert (SBN 265803)
kschubert@sjk.law
SCHUBERT JONCKHEER & KOLBE LLP
Three Embarcadero Center, Suite 1650
San Francisco, California 94111
Tel: 415.788.4220
Fax: 415.788.0161

Attorneys for Plaintiffs and the Putative Classes

CERTIFICATE OF SERVICE

I, Nina Eisenberg, an attorney, hereby certify that on July 10, 2017, I served the above and foregoing ***First Consolidated Class Action Complaint*** by causing a true and accurate copy of such paper to be filed and transmitted to all counsel of record via the Court's CM/ECF electronic filing system.

/s/ Nina Eisenberg